**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MASSACHUSETTS**
**EASTERN DIVISION**

**CHARLES MCCURDY**, on behalf of himself and on behalf of all others similarly situated,

Plaintiff,

v.

**GREYLOCK MCKINNON ASSOCIATES INC.,**

Defendant.

Case No. _____

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Charles McCurdy ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through his undersigned counsel, files this Class Action Complaint against Greylock McKinnon Associates Inc. ("Greylock" or "Defendant") and alleges the following based on personal knowledge of facts, upon information and belief, and based on the investigation of his counsel as to all other matters.

## I. NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Greylock for its negligent failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") culminating in a massive and preventable data breach (the "Data Breach" or "Breach"). As a result of Greylock's insufficient data security, cybercriminals easily infiltrated Greylock's inadequately

protected computer systems and ***stole*** the Private Information of Plaintiff and the Class (approximately 341,650 individuals).[1]

2. According to Greylock, on May 30, 2023, Greylock detected unusual activity in its internal network.[2]

3. After an investigation, it was determined that Greylock was the subject of a ransomware attack.[3]

4. The cybercriminal group behind the ransomware attack obtained copies of files from Greylock's systems.[4]

5. Greylock openly admits that the Data Breach resulted in the exposure and exfiltration of several files that included the Private Information of Plaintiff and the Class.

6. The types of Private Information compromised in the Data Breach included: names, Social Security numbers, dates of birth, mailing addresses, telephone numbers, Medicare beneficiary providers or Health Insurance Claim Numbers, driver's license numbers, state identification numbers, healthcare provider and prescription information, health insurance claims and policy/subscriber information, health benefits and enrollment information, and medical history/notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.).[5]

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/865575ae-973b-4430-a06c-d780da040c74.shtml.
[2] *See* Ex. 1 (Notice of Breach Letter).
[3] *Id.*
[4] *Id.*
[5] *Id.*

7. Due to Defendant's negligence, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

8. Now, for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

9. Plaintiff brings this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

## II. THE PARTIES

10. Plaintiff **Charles McCurdy** is an individual domiciled in Houston, Texas. Plaintiff received the Notice of Breach Letter attached hereto as **Exhibit 1**, from the U.S. Department of Justice ("DOJ"), notifying him that his Private Information was contained in the files that were exfiltrated from Greylock's systems.

11. Defendant **Greylock McKinnon Associates Inc.** is a corporation organized under the laws of Massachusetts with its headquarters and principal place of business located at 75 Park Plaza, 4th Floor, Boston, Massachusetts 02116.

## III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than Defendant.

13. This Court has personal jurisdiction over Defendant because Defendant is incorporated and/or has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

14. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District.

## IV. FACTUAL ALLEGATIONS

### A. Greylock and its Collection of Plaintiff's and the Class's Private Information.

15. Greylock is a consulting firm that provides litigation support services in civil litigation matters. [6]

16. GMA works with domestic and international corporations ranging from Fortune 100 companies to small regional companies and state and federal governmental agencies, as well as with many major law firms in the United States and abroad.

[6] https://www.gma-us.com/.

17. The Private Information of Plaintiffs and the Class was acquired by the DOJ as part of a civil litigation matter.[7]

18. In turn, Greylock received Plaintiff's and the Class's Private Information in its provision of services to the DOJ in support of that matter.[8]

19. Greylock McKinnon Associates employs more than 28 people and generates approximately $5 million in annual revenue.[9] This makes it apparent Greylock could have implemented adequate data security prior to the Breach but deliberately chose not to.

20. In the ordinary course of business, Greylock receives the Private Information of individuals, such as Plaintiff and the Class, from its customers.

21. Greylock obtains, collects, uses, and derives a benefit from the Private Information of Plaintiff's and Class Members. Greylock uses the Private Information it collects to provide services, making a profit therefrom. Greylock would not be able to obtain revenue if not for the acceptance and use of Plaintiff's and the Class's Private Information.

22. By collecting Plaintiff's and the Class's Private Information, Greylock assumed legal and equitable duties to Plaintiff and the Class to protect and safeguard their Private Information from unauthorized access and intrusion.

23. However, Greylock failed to protect Plaintiff's and the Class's Private Information.

24. As a result, Plaintiff's and Class Members' Private Information was accessed and stolen from Greylock's inadequately secured computer network in a massive and preventable Data Breach.

---

[7] *Id.*
[8] *Id.*
[9] https://www.jdsupra.com/legalnews/greylock-mckinnon-notifies-341-650-of-6232827/#:~:text=Greylock%20McKinnon%20Associates%20employs%20more,%245%20million%20in%20annual%20revenue.

**B. Greylock's Massive and Preventable Data Breach.**

25. According to the Notice of Breach Letter mailed to Plaintiff and the Class, on May 30, 2023, Greylock discovered it had experienced a ransomware attack affecting several of its systems.[10]

26. Greylock's initial investigation determined that the group behind the ransomware attack obtained copies of files from Greylock's systems.[11]

27. Specifically, the Notice of Breach Letter confirmed that the Data Breach "resulted in the exposure and exfiltration of files" in Greylock's possession.[12]

28. The Private Information stolen in the Data Breach included a plethora of information such as: names, Social Security numbers, dates of birth, mailing addresses, telephone numbers, Medicare beneficiary providers or Health Insurance Claim Numbers, driver's license numbers, state identification numbers, healthcare provider and prescription information, health insurance claims and policy/subscriber information, health benefits and enrollment information, and medical history/notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.).[13]

29. Despite learning of the Data Breach on May 30, 2023, notice of the data breach was not issued to Plaintiff until April 5, 2024.[14]

[10] *See* Ex. 1.
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*

30. Defendant acknowledged the harm that would befall Plaintiffs in the Class in the Notice of Breach Letter because it encouraged individuals to enroll in credit monitoring services and obtain their credit reports.[15]

31. Defendant's actions represent a flagrant disregard of the rights of Plaintiff and the Class, both as to privacy and property.

32. Greylock makes ***no*** assurances to Plaintiff and the Class that it attempted to regain Plaintiff's and the Class's data from the threat actor or paid the ransom demand.

33. As such, Plaintiff and the Class are at an imminent and impending risk of identity theft and fraud.

### C. Cyber Criminals Will Use Plaintiff's and the Class's Private Information to Defraud them.

34. Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

35. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[16]

36. For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of

[15] *Id.*

[16] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

identity theft.[17] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

37. Medical-related identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013[,]" which is more than identity thefts involving banking and finance, the government and the military, or education.[18]

38. "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place."[19] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[20]

39. When cybercriminals manage to steal health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Plaintiff and Class Members are exposed.

40. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

---

[17] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[18] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

[19] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015) https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat..

[20] *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015*, PRICEWATERHOUSECOOPERS (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[21]

(Emphasis added.)

41. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[22]

42. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running targeted cyberattacks against companies like Greylock is to get ransom money and/or information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein.

43. A social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[23]

44. PHI is even more valuable on the black market than PII.[24]

45. According to the Center for Internet Security, "[t]he average cost of a data breach incurred by a non-healthcare related agency, per stolen record, is $158. For healthcare agencies the cost is an average of $355. Credit card information and PII sell for $1-$2 on the black market, but PHI can sell for as much as $363 according to the Infosec Institute. This is because one's

---

[21] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[22] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at https://www.gao.gov/products/gao-07-737.
[23] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web* (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.
[24] *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector.

personal health history, including ailments, illnesses, surgeries, etc., can't be changed, unlike credit card information or Social Security Numbers."[25]

46. "PHI is valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can also be used to create fake insurance claims, allowing for the purchase and resale of medical equipment. Some criminals use PHI to illegally gain access to prescriptions for their own use or resale."[26]

47. "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[27]

48. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, ***they will use it***.[28]

49. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

---

[25] *Id.*
[26] *Id.*
[27] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[28] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.
[29] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO (July 5, 2007), available at https://www.gao.gov/products/gao-07-737.

50. For instance, with a stolen social security number, which is part of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[30]

51. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[31]

52. Defendant made a limited offer of identity monitoring to Plaintiff and the Class. But such coverage is woefully inadequate and will not fully protect Plaintiff from the damages and harm caused by its failures.

53. The full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

54. Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Greylock's gross negligence.

55. Furthermore, identity monitoring only alerts someone to the fact that they have **already been the victim of identity theft** (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[32] Nor can an identity monitoring service remove personal information from the dark web.[33]

---

[30] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[31] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), *available at* https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

[32] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

[33] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

56. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[34]

57. As a direct and proximate result of the Data Breach Plaintiff and the Class have been damaged and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

58. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

59. Plaintiff and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property including Private Information;

c. Improper disclosure of their Private Information;

[34] *Id.*

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their Private Information;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breaches;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

60. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's Private Information.

61. Plaintiff and Class Members also have an interest in ensuring that their personal information that was provided to Greylock is removed from all Greylock servers, systems, and files.

62. Given the kind of Private Information Greylock made accessible to hackers, however, Plaintiff is certain to incur additional damages. Because identity thieves have their Private Information, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[35]

63. None of this should have happened because the Data Breach was entirely preventable.

**D. Defendant was Aware of the Risk of Cyberattacks.**

64. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[36] Yahoo,[37] Marriott International,[38] Chipotle,

[35] *What happens if I change my Social Security number*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[36] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last visited Oct. 9, 2023).

[37] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[38] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

Chili's, Arby's,[39] and others.[40]

65. Greylock should certainly have been aware, and indeed was aware,[41] that it was at risk of a data breach that could expose the Private Information that it collected and maintained, especially with the rise of legal industry data breaches.[42]

66. Greylock's assurances of maintaining high standards of cybersecurity make it evident that Greylock recognized it had a duty to use reasonable measures to protect the PII that it collected and maintained.

67. Greylock was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

**E. Greylock Could Have Prevented the Data Breach.**

68. Data breaches are preventable.[43] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[44] She added that "[o]rganizations that collect, use, store, and share sensitive

[39] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[40] *See, e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[41] https://Greylockok.com/notice-of-privacy-practices;https://Greylockok.com/landing/cyber-event.

[42] *See* https://www.darkreading.com/cyberattacks-data-breaches/law-firms-face-a-more-dangerous-threat-landscape.

[43] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.

[44] *Id.* at 17.

personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[45]

69. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[46]

70. In a Data Breach like this, many failures laid the groundwork for the Breach.

71. The FTC has published guidelines that establish reasonable data security practices for businesses.

72. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[47]

73. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.

74. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

---

[45] *Id.* at 28.
[46] *Id.*
[47] *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

75. According to information and belief, Greylock failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines.

76. Upon information and belief, Greylock also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

77. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[48]

78. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

[48] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[49]

79. Further, to prevent and detect malware attacks, including the malware attacks that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

[49] *Id.* at 3–4.

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[50]

[50] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at https://www.cisa.gov/news-events/news/protecting-against-ransomware.

80. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[51]

81. Given that Defendant was storing the Private Information of millions of individuals, Defendant could have and should have implemented all of the above measures to prevent and detect cyberattacks.

82. Specifically, among other failures, Greylock had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[52]

83. Moreover, it is well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed.

84. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary Private Information, saying simply: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[53] Greylock, rather than following this basic standard of care, kept thousands of individuals' unencrypted Private Information indefinitely.

---

[51] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[52] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, FORTRA (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption (last visited Oct. 9, 2023).

[53] *Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

85. In sum, the Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all Private Information.

86. Further, the scope of the Data Breaches could have been dramatically reduced had Greylock utilized proper record retention and destruction practices.

**F. Plaintiff McCurdy's Individual Experience**

87. Plaintiff's Private Information was obtained by the DOJ as part of a civil investigation and related litigation matter and the DOJ provided Plaintiff's Private Information to Greylock in support of that matter.[54]

88. By accepting Plaintiff's Private Information, Defendant agreed to safeguard it and protect it from unauthorized access and delete it after a reasonable time.

89. Defendant was in possession of Plaintiff's Private Information before, during, and after the Data Breach.

90. As a result of the Data Breach, Plaintiff's name, Social Security number, date of birth, mailing address, telephone number, Medicare beneficiary providers or Health Insurance Claim Numbers, driver's license number, state identification number, healthcare provider and prescription information, health insurance claims and policy/subscriber information, health benefits and enrollment information, and/or medical history/notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.) were exfiltrated and stolen in the Data Breach.

91. As a direct and traceable result of the Data Breach, Plaintiff has been forced to spend hours dealing with and responding to the direct consequences of the Data Breach, which

---

[54] *See* Ex. 1.

includes researching the Data Breach, reviewing, and monitoring his accounts for fraudulent activity, reviewing his credit reports, and researching credit monitoring services. In total, Plaintiff estimates he has already spent over two (2) hours responding to the Data Breach. However, this is not the end. Plaintiff will be forced to expend additional time to review his credit reports and monitor his accounts for the rest of his life. This is time spent at Defendant's direction, which has been lost forever and cannot be recaptured.

92. Plaintiff places significant value in the security of his Private Information and does not readily disclose it. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

93. As a direct and traceable result of the Data Breach, Plaintiff suffered actual damages such as: (1) lost time related to monitoring his accounts and credit reports for fraudulent activity; (2) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (3) loss of the benefit of the bargain because Defendant did not adequately protect his Private Information; (4) emotional distress because identity thieves now possess his first and last name paired with his Social Security number and other sensitive information; (5) exposure to increased and imminent risk of fraud and identity theft now that his Private Information has been accessed; (6) the loss in value of his Private Information due to his Private Information being in the hands of cybercriminals who can use it at their leisure; and (7) other economic and non-economic harm.

94. Plaintiff has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach and the fact that Defendant admits data was stolen in the Data

Breach.[55]

95. Knowing that thieves intentionally targeted and stole his Private Information, including his Social Security number, and knowing that his Private Information is in the hands of cybercriminals has caused great anxiety beyond mere worry. Specifically, Plaintiff has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that his Private Information has been stolen.

96. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff's, and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

## V. CLASS ACTION ALLEGATIONS

97. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

98. Plaintiff brings this action against Greylock on behalf of himself and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> **All persons whose Private Information was compromised in the Greylock Data Breach occurring in or around May 2023.**

99. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

[55] *Id.*

100. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

101. Plaintiff anticipates the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

102. The proposed Class meets the requirements of Federal Rule of Civil Procedure 23.

103. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. The total number of individuals affected is more than 300,000 people.

104. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Greylock's uniform misconduct. Greylock's inadequate data security gave rise to Plaintiff's claims and are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of Greylock.

105. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

106. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Greylock's wrongdoing. Even if Class members could

afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

107. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Private Information;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Private Information, and whether it breached this duty;

d. Whether Greylock breached its duties to Plaintiff and the Class;

e. Whether Greylock failed to provide adequate cyber security;

f. Whether Greylock knew or should have known that its computer and network security systems were vulnerable to cyber-attacks;

g. Whether Greylock's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Greylock was negligent in permitting unencrypted Private Information off vast numbers of individuals to be stored within its network;

i. Whether Greylock was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breaches to include former employees and business associates;

j. Whether Greylock breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their Private Information;

k. Whether Greylock failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

l. Whether Greylock continues to breach duties to Plaintiff and the Class;

m. Whether Plaintiff and the Class suffered injury as a proximate result of Greylock's negligent actions or failures to act;

n. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Greylock's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

## VI. CAUSES OF ACTION

### FIRST CAUSE OF ACTION
### NEGLIGENCE
### (On Behalf of Plaintiff and the Class)

108. Plaintiff incorporates foregoing paragraphs as though fully set forth herein.

109. Greylock solicited, gathered, and stored the Private Information of Plaintiff and Class Members.

110. Upon accepting and storing the Private Information of Plaintiff and Class members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiff and Class

members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiff and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

111. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

112. Because of this special relationship, Defendant required Plaintiff and Class members to provide their Private Information, including names, Social Security numbers, and other Private Information.

113. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class members in its possession was only used for the provided purpose and that Defendant would destroy any Private Information that it was not required to maintain.

114. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness.

115. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiff's and Class members' Private Information from being foreseeably accessed, and its improper retention of Private Information it was not required to maintain, Defendant negligently failed to observe and perform its duty.

116. Plaintiff and Class members did not receive the benefit of the bargain with

Defendant, because providing their Private Information was in exchange for Defendant's implied agreement to secure and keep it safe and to delete it once no longer required.

117. Defendant was aware of the fact that cybercriminals routinely target healthcare entities through cyberattacks in an attempt to steal patient and employee Private Information. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

118. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

119. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

120. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and

practices to ensure that Plaintiff's and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' Private Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and

d. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

121. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the Private Information that Plaintiff and the Class had entrusted to it.

122. Plaintiff's injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

123. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's Private Information;

d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

e. Failing to promptly notify Plaintiff and Class members of the Data Breaches that affected their Private Information.

124. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

125. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

126. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class members while it was within Defendant's possession and control.

127. Further, through its failure to provide timely and clear notification of the Data Breaches to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

128. Plaintiff and Class members could have taken actions earlier had they been timely notified of the Data Breaches.

129. Plaintiff and Class members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breaches more quickly.

130. Plaintiff and Class members have suffered harm from the delay in notifying them of the Data Breaches.

131. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiff and Class members have suffered, as Plaintiff have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breaches, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

132. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

133. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

**SECOND CAUSE OF ACTION**
**NEGLIGENCE *PER SE***
**(On Behalf of Plaintiff and the Class)**

134. Plaintiff incorporates foregoing paragraphs as though fully set forth herein.

135. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and the Class.

136. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

137. Defendant gathered and stored the Private Information of Plaintiff and the Class as part of their business which affects commerce.

138. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

139. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class members' Private Information, and by failing to provide prompt notice without reasonable delay.

140. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

141. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

142. The harm that occurred as a result of the Data Breaches is the type of harm the FTC Act was intended to guard against.

143. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Private Information.

144. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breaches expeditiously and/or as soon as practicable to Plaintiff and the Class.

145. Defendant's violations of the FTC Act constitute negligence *per se*.

146. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breaches, as alleged above.

147. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

148. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

**THIRD CAUSE OF ACTION**
**BREACH OF THIRD-PARTY BENEFICIARY CONTRACT**
**(On Behalf of Plaintiff and the Class)**

149. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

150. Plaintiffs and Class Members are intended third-party beneficiaries of contracts entered into between DOJ and Greylock (the "contracting parties"), including a contract entered into before the Data Breach to provide services (the "Contract").

151. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

152. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients Plaintiffs and Class Members would be harmed.

153. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

154. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

155. Accordingly, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial.

**FOURTH CAUSE OF ACTION**
**UNJUST ENRICHMENT**
**(On Behalf of Plaintiff and the Class)**

156. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

157. Plaintiff alleges this claim in the alternative to his breach of third-party beneficiary contract claim.

158. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have had their Private Information protected with adequate data security.

159. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

160. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

161. Defendant acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

162. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information at Defendant.

163. Plaintiff and Class Members have no adequate remedy at law.

164. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

165. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

166. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

167. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

**FIFTH CAUSE OF ACTION**
**DECLARATORY AND INJUNCTIVE RELIEF**
**(On Behalf of Plaintiff and the Class)**

168. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

169. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

170. As previously alleged, Plaintiff and members of the Class are entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the Private Information collected from Plaintiff and the Class.

171. Defendant owed and still owes a duty of care to Plaintiff and Class members that require it to adequately secure Plaintiff's and Class members' Private Information.

172. Upon reason and belief, Defendant still possesses the Private Information of Plaintiff and the Class members.

173. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class members.

174. Since the Data Breach, Defendant has not yet announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breaches to occur and go undetected and, thereby, prevent further attacks.

175. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattack.

176. Actual harm has arisen in the wake of the Data Breaches regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

177. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breaches to meet Defendant's contractual obligations and legal duties.

178. Plaintiff and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f. Ordering that Defendant conduct regular database scanning and security checks; and

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

## VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

## VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: April 17, 2024.

Respectfully submitted,

*/s/ Christina Xenides*
Christina Xenides, Bar No. 677603
Mason A. Barney*
Tyler Bean*
**SIRI & GLIMSTAD LLP**
SIRI & GLIMSTAD LP
1005 Congress Avenue, Suite 925-C36
Austin, TX 78701
Tel: (512) 265-5622
cxenides@sirillp.com
mbarney@sirillp.com
tbean@sirillp.com

William B. Federman, OBA # 2853
Kennedy M. Brian, OBA # 34617
*(Pro hac vice applications forthcoming)*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
E:wbf@federmanlaw.com
E: kpb@federmanlaw.com

*Counsel for Plaintiff and the Putative Class*
**Pro hac vice* forthcoming